Trabajo Fin de Grado

Título del trabajo: Seguridad y privacidad en el uso de las tics aplicadas al marketing online.

Title: Safety and privacy using TICs within online marketing.

Autor/es

Ignacio Rodrigo Boned

Director/es

Francisco Sobrino Bescós

Facultad / Escuela: Facultad de Economía y Empresa

Año: 2020

0.-INFORMACIÓN Y RESUMEN

0.1 Información General

Autor del Trabajo: Ignacio Rodrigo Boned

Director del Trabajo: Francisco Sobrino Bescós

Título del Trabajo: Seguridad y privacidad en el uso de las tics aplicadas al marketing online. (Safety and privacy using TICs within online marketing).

Titulación del Trabajo: Graduado en Marketing e Investigación de Mercados (450).

0.2 Resumen Ejecutivo

El Marketing Digital a día de hoy es una estrategia imprescindible para las empresas ya que ofrece una gran oportunidad de crecimiento, posicionamiento, captación de clientes y ventas. Esto conlleva que cada vez más empresas de pequeño tamaño, en particular los comercios tradicionales y autónomos, situados muchas veces en entornos rurales, quieran vender sus productos y servicios a través del comercio electrónico.

Una Agencia de Marketing Online facilita la incorporación de sus negocios a la red de Internet mediante la creación de páginas webs, creación de aplicaciones de Marketplace y/o presencia en redes sociales. Todo ello conlleva una serie de cambios en la gestión de los negocios y adicionalmente nuevos requisitos legales que se deben cumplir para estar presentes en las citadas redes. En particular la seguridad y privacidad de los datos personales que se obtienen por cualquier fuente durante las transacciones debe gestionarse adecuadamente, cumpliendo las obligaciones impuestas por la Unión Europea y que han sido transpuestas posteriormente a nuestro derecho interno. Este hecho cobra una importancia significativa con la entrada en vigor del Reglamento Europeo 2016/79 y la publicación de la Ley Orgánica 3/2018. Los incumplimientos y las importantes sanciones que se derivan de una mala gestión de los datos personales puede llevar incluso al cese de la actividad de una empresa.

En este trabajo se documenta un **Sistema de Gestión de la Seguridad para el Tratamiento de Datos Personales** en una Agencia de Marketing Online para que cumpliendo lo que en él se establece la empresa tenga el convencimiento de que sus prácticas con la gestión de los datos personales son correctas y ajustadas al ordenamiento jurídico vigente. En él se recogen las medidas técnicas y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los sistemas de información de la agencia **Smarketing4all, S.L.**

INDICE

1.-INTRODUCCIÓN

El presente documento tiene por objeto definir y desarrollar un **Sistema de Gestión de la Seguridad para el Tratamiento de Datos Personales** en una empresa con razón social **Smarketing4all, S.L** que nos permita cumplir con los requisitos legales establecidos tras la entrada en vigor de la nueva Ley Orgánica 3/2018 del 5 de Diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, así como lo dispuesto artículo 30 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En él se establece que cada Responsable del Tratamiento de Datos llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad, en el que se recogerá una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1 de dicho Reglamento.

1.1 Descripción de la empresa

Smarketing4all, S.L. es una Agencia de Marketing Digital que ofrece servicios de asesoramiento y apoyo externo a empresas y autónomos en lo relacionado con la planificación, implantación y control de las actividades de marketing.

Nuestros Clientes potenciales son microempresas y pequeñas empresas locales, principalmente comercios que, debido a su tamaño, no suelen disponer de un departamento específico de marketing. Nosotros les ayudamos a definir y desarrollar su proyecto en Internet, a posicionarlo en buscadores y a difundirlo en redes sociales.

Entre los servicios que proporcionamos están los siguientes:

- **Desarrollo y diseño Web**, es decir determinar la apariencia del sitio web e implementar sus funciones.
- **Analítica Digital,** mediante la cual la empresa podrá saber las estadísticas y los resultados de su sitio online permitiendo su optimización.
- **Inbound Marketing** o marketing de contenidos a través del seguimiento de leads (contactos), mejorando el posicionamiento en los buscadores y la imagen de una marca mediante contenidos útiles y personalizados. Estas acciones tienen como objetivo transformar los visitantes en leads y convertirlos en Clientes.

- **Análisis del Retorno de Inversión (ROI),** que permite medir la rentabilidad de una estrategia al evaluar si la inversión se está convirtiendo en ganancia.
- **E-mail Marketing**, mediante el envío de correos a la base de datos de los Clientes de una empresa con mensajes comerciales, promociones, entre otras cosas, y así tenerlos al tanto de todas las acciones que se están realizando.
- **Social Media Marketing**, mediante la gestión de las redes sociales de la empresa, como Facebook, Twiter, Instagram, etc., y diseñando su contenido para generar tráfico es estas plataformas. Estos medios se utilizan también para invertir en publicidad y llegar con más precisión al público objetivo
- **Posicionamiento SEO** (Search Engine Optimization). optimizamos las búsquedas para posicionar a la empresa en un buen lugar en los buscadores, como Google, de manera orgánica (no pago).
- **Posicionamiento SEM** (Search Engine Marketing), diseñamos y gestionamos campañas de anuncios y enlaces patrocinados en los motores de búsqueda.

Nuestro equipo está formado por 4 socios directores y otros colaboradores que abarcan todas las especialidades descritas, constituyendo un equipo flexible, colaborativo y con clara orientación al Cliente.

Mediante las **acciones** de Marketing Digital que proporcionamos a nuestros Clientes conseguimos los siguientes **objetivos**:

- **Captar tráfico**, es decir, crear contenido enfocado al objetivo al que se desea llegar, para fomentar las visitas.
- **Activar la respuesta** o interacción por parte de la audiencia digital.
- **Convertir y generar** ventas, transacciones, registros, descargas.
- **Fidelizar al Cliente**, ya que es mucho más fácil retenerlo que convencer a uno nuevo

1.1 Datos de la empresa

Razón Social: Smarketing4all, S.L (en adelante SMK)

Dirección: Centro ETOPIA. Avda. Ciudad de Soria, 8. 50010 Zaragoza.

Página web: www.smarketing4all.com

email general: smarketing4all@smarketing.com

email específico: lopdp@smarketing.com

2.-LEGISLACIÓN APLICABLE.

- **Ley Orgánica 3/2018**, de 5 de Diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (BOE nº294, de 6 de Diciembre de 2018) (LOPDPGDD).(deroga la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal)
- **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD).
- **Ley 34/2002**, de 11 de Julio, de Servicios de la Sociedad de la Información de Comercio Electrónico (LSSI).

Con objeto de facilitar la trazabilidad entre la legislación aplicable y el **SGSTDP** se ha elaborado una **Tabla de Equivalencias** (ver Anexo I).

3.-DEFINICIONES Y ABREVIATURAS

3.1 Definiciones.

A continuación, se indican las definiciones de los términos más usuales utilizados en el presente documento y contenidas en la legislación aplicable :

«Datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

«Tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

«Elaboración de Perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

«Fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

«Responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

«Encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

«Destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

«Tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

«Consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

«Violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

«Datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

«Datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

«Datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

«Empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.

«Autoridad de Control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51 de Reglamento (UE) 2016/679.

Otras **definiciones específicas** de este Sistema son las siguientes:

«Interesado: Persona física titular de los datos que sean objeto del tratamiento.

«Incidencia o Brecha de Seguridad»: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos personales.

«Delegado de Protección de Datos»: Persona o personas a las que el responsable del tratamiento ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables

«Sistema de Tratamiento»: Modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

«Usuario»: Sujeto o proceso autorizado para acceder a datos de carácter personal o recursos.

3.2 Abreviaturas

- **SMK:** Smarketing4all, S.L
- **RGPD:** Reglamento (UE) 2016/679.
- **LOPDPGDD**: Ley Orgánica 3/2018.
- **LSSI:** Ley 34/2002.
- **AEPD:** Agencia Española de Protección de Datos.
- **SGSTDP**: Sistema de Gestión de la Seguridad para el Tratamiento de Datos Personales.
- **RTD:** Responsable del Tratamiento de Datos**.**
- **DPD:** Delegado de Protección de Datos.

4.-DECLARACIÓN SOBRE PRIVACIDAD

SMK como Responsable del Tratamiento de Datos, establece en esta **Declaración de Privacidad** las finalidades del tratamiento de datos personales en base al principio de responsabilidad proactiva así como los criterios para optimizar la gestión de la seguridad y protección de los datos de forma que resulte útil, ágil y efectiva y nos permita alcanzar los objetivos que la legislación requiere.

Para ello, asumimos y nos comprometemos a **cumplir con los siguientes principios** que el RGPD establece en su artículo 5:

1. Los datos personales deben ser tratados de **manera lícita, legal y transparente** en relación con el interesado.
2. Los datos deben recogerse con fines **determinados, explícitos y legítimos**, y no serán tratados ulteriormente de manera incompatible con dichos fines.
3. Los datos deben ser **adecuados, pertinentes y limitados** a lo necesario en relación con los fines para los que son tratados.
4. Los datos deben de ser **exactos**, y cuando sea necesario, actualizados.
5. Los datos deben ser mantenidos de forma que se permita la identificación de los interesados durante **no más tiempo** que el necesario para que los fines del tratamiento.
6. Los datos deben ser tratados de manera que se garantice la **integridad y la confidencialidad** de los interesados.

La Dirección General de **SMK** nombra a un **Delegado del Tratamiento de Datos** que además de otras responsabilidades en la empresa, deberá garantizar el cumplimiento de los principios aquí definidos, así como mantener al día nuestr**a Política de Privacidad**, nuestra **Política de Cookies** así como la información legal que aparece en nuestra página web. Para ello se aprueba este documento que constituye un sistema en el que se basan las actividades del tratamiento de la empresa y que periódicamente será auditado por personal externo cualificado para asegurarnos de su cumplimiento.

Fdo.:	Director de Marketing-IT Delg del Tratamiento de Datos	Fdo. El Director General Resp. del Tratamiento de Datos

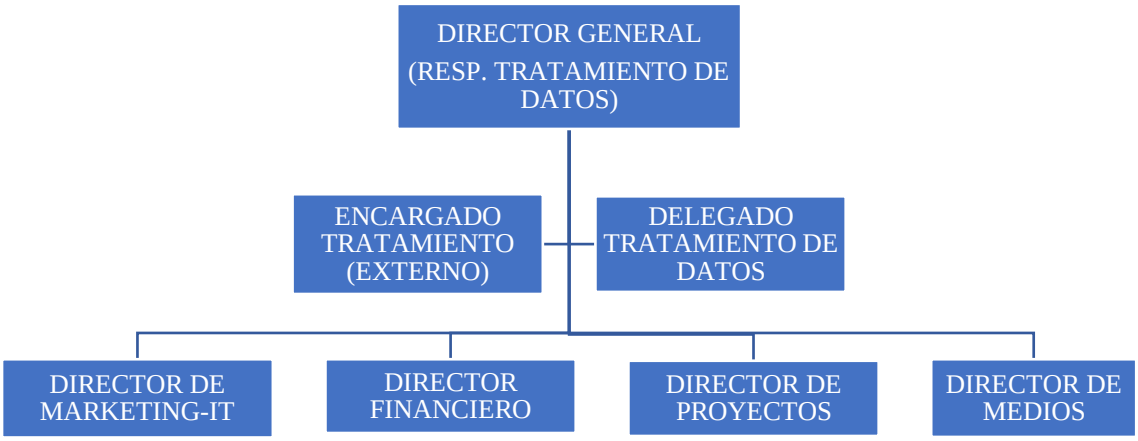
5.-SISTEMA DE GESTIÓN DE LA SEGURIDAD.

5.1 Ámbito de Aplicación

El Sistema de Gestión se ha desarrollado para facilitar el cumplimiento de la legislación aplicable a la empresa en materia de Protección de Datos El presente documento será de aplicación a los tratamientos de datos de carácter personal que se hallan bajo la responsabilidad de **SMK**, que en adelante denominaremos **Responsable del Tratamiento de Datos (RTD)**, así como los locales, sistemas de información, soportes y equipos empleados para el tratamiento de dichos datos, que deban ser protegidos conforme a lo establecido en la normativa vigente.

5.2 Organización y Responsabilidades

La organización de **SMK**, en relación con el Sistema, se describe en el siguiente Organigrama:



Asumen las siguientes **funciones y responsabilidades**:

Director General- Responsable del Tratamiento de Datos

Además de las funciones y responsabilidades inherentes a su cargo es la persona **Responsable del Tratamiento de Datos** y como tal tiene las responsabilidades que derivan de este Sistema y las definidas en los artículos 24 y 25 del **RGPD** y artículo 28 de la **LOPDPGDD,** resaltando la relativa a la determinación de las medidas técnicas y organizativas apropiadas que se deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con la legislación aplicable.

Encargado del Tratamiento (Externo)

En el caso de que la empresa decida **subcontratar** la figura del Encargado de Tratamiento de Datos es necesario que se firme un contrato por ambas partes detallando las funciones y responsabilidades de ambas empresas, recogiendo las obligaciones que marca la legislación, art. 28 y 29 del **RGPD**.

Delegado del Tratamiento de Datos

En nuestro caso es el **Director de Marketing-IT** quien además de las funciones y responsabilidades inherentes a su cargo asume las relacionadas con este Sistema y las recogidas en el artículo 39 del **RGPD**,

El **RTD** dispone de un plazo de 10 días para comunicar su nombramiento y/o cese a la **AEPD**.

Otros Directores y Usuarios:

El resto de Directores de **SMK** así como cualquier otro colaborador que preste sus servicios en **SMK,** tienen la consideración de Usuarios y como tales adquieren las obligaciones que emanan de este Sistema:

Todo el personal de la empresa está obligado a firmar un **Compromiso de Confidencialidad** en el momento de su incorporación y antes de acceder a datos personales, poniendo a su disposición este documento para su conocimiento y aplicación en lo que le afecte, estando sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

5.3 Recursos protegidos del SGSPD

Se entiende por **recurso protegido** *"cualquier parte componente del sistema de información"*; esto es, los ficheros referidos en el apartado siguiente, así como los programas informáticos, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Los recursos por tratarse de un medio directo o indirecto de acceso a los Ficheros, dependiendo de si se realiza un tratamiento automatizado o manual del mismo, deberán ser controlados e incluyen:

- Los locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan.
- Los puestos de trabajo desde los que se pueda tener acceso al Fichero.
- Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos.
- El servidor y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el Fichero.
- Los armarios y archivadores donde se guarden los ficheros no automatizados, cuando no estén siendo tratados.

5.4 Documentación del Sistema

El **SGPD** está formado por los siguientes documentos:

-El Manual de Privacidad aquí desarrollado.

-Los registros derivados de las actividades de Tratamiento de Datos.

-Las Políticas de Privacidad y de Cookies.

-Las listas, comunicaciones y reclamaciones de interesados, registros de incidencias, procedimientos administrativos, informes de evaluación, datos personales y cualquier documento relacionado con la gestión de este Sistema.

Todos los registros y documentos indicados serán archivados por el **DPD** por un período mínimo de 5 años, excepto las Políticas y los registros de actividades de tratamiento que se mantendrán siempre actualizados en su última revisión.

5.5 Revisión del SGSDP

Este documento de obligado cumplimiento para todo el personal con acceso a los sistemas de información que traten datos de carácter personal.

El **DPD** tiene la responsabilidad de **mantenerlo actualizado y revisarlo**, si procede, en el caso de que se produzcan cambios en los sistemas de información, en el sistema de tratamiento empleado, en la Organización, en las disposiciones vigentes en materia de seguridad de datos personales y como consecuencia de la realización de las evaluaciones periódicas descritas en el apartado 11 de este documento.

6.-TRATAMIENTO DE LOS DATOS.

6.1. Análisis de Riesgos y Evaluación del Impacto.

El **RGPD** exige al **RTD** la realización de un análisis de riesgos y evaluaciones de impacto con el fin de llevar a cabo una gestión de los riesgos para los derechos y libertades de las personas físicas Este análisis se documentará **antes de realizar** cualquier actividad de tratamiento.

El Análisis de Riesgos viene a cubrir los dos aspectos que requiere el **RGPD**, es decir la responsabilidad proactiva y el enfoque del tratamiento desde el riesgo. El tipo de análisis variará en función de:

-Los tipos del tratamiento.

-La naturaleza de los datos.

-El nº de interesados afectados.

-La cantidad de los tratamientos que realizamos.

Este análisis nos indicará si las medidas que disponemos son suficientes para garantizar la confidencialidad, la disponibilidad y la integridad de la información y de los sistemas de información de nuestra empresa.

La Evaluación de Impacto en la Protección de Datos Personales (EIPD) es una herramienta con carácter preventivo que debe realizar el **RTD** para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.

En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

Para realizar este análisis nos basamos en la herramienta **GESTIONA_EIPD** y en los documentos publicado por la AEPD (ver Bibliografía documentos nº

6.2 Tipos de datos a tratar

Los tratamientos realizados por **SMK** se resumen en la siguiente tabla

NOMBRE DEL FICHERO	TIPO DE TRATAMIENTO
CLIENTES	Manual y automático
CLIENTES POTENCIALES	Manual y automático (web SMK, landing pages, anuncios, web de Clientes).
PROVEEDORES	Manual y automático
RECURSOS HUMANOS	Manual y automático

En ambos casos los datos van a ser tratados directamente por **SMK**, no existiendo como se ha indicado en el apartado 5.2 la figura del Encargado del Tratamiento.

Quedan **prohibidos** en nuestra empresa el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéricos, datos biométricos, dirigidos a identificar de manera univoca a una persona física, datos relativos a la vida sexual o a las orientaciones sexuales de una persona física o datos personales relativos a condenas e infracciones penales.

6.3 Finalidades y Legitimación

Los datos obtenidos serán utilizados por nuestra empresa para las siguientes **finalidades**:

-Envío de comunicaciones de carácter comercial.

-Para la prestación del servicio contratado.

-Para el cumplimiento de obligaciones legales.

Las bases de la **legitimación** son las siguientes:

-Consentimiento del interesado.

-Tratamiento necesario para la ejecución de un contrato.

-Interés legítimo.

6.4 Registro de las Actividades de Tratamiento

Aunque el registro de las actividades de tratamiento no es obligatorio para empresas de menos de 250 empleados (excepto si contienen datos que puedan entrañar riesgo para los derechos y libertades de las personas o datos especiales), el **DPD** deberá elaborar un **Registro del Tratamiento de Datos** de cada fichero (ver Anexo II), informático y en papel, con los datos allí recogidos y que incluyen los indicados en el art. 30 de **RGPD**. El registro estará siempre actualizado y a disposición de la **Autoridad de Control** (AEPD).

El **RTD** está obligado a **bloquear los datos** cuando proceda a su rectificación o supresión. El bloqueo consiste en la identificación y reserva de los mismos, impidiendo su tratamiento y visualización, excepto para la puesta a disposición de los mismos a las Administraciones Públicas que lo requieran y por el plazo que lo soliciten. Transcurrido dicho plazo, el **DPD** procederá a su destrucción.

6.5 Transferencias Internacionales de Datos

No está previsto comunicar ningún dato fuera del Espacio Económico Europeo. En el caso de que en algún momento se produjera este hecho a través de terceros, se deberá tener en cuenta lo establecido en los artículos 40 al 43 de la **LOPDPGDD.**

6.6 Otros Tratamientos

Personas fallecidas.

Las personas vinculadas al fallecido por razones familiares o sus herederos podrán dirigirse al **RTD/DTD** al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión, a no ser que el fallecido lo hubiese prohibido expresamente.

Menores de edad.

El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea **mayor** de 14 años.

En el caso de **menores** de 14 años sólo será lícito si consta también el consentimiento del titular de la patria potestad o tutela.

7.-DERECHOS E INFORMACIÓN A LOS INTERESADOS.

Los datos personales pueden obtenerse de dos maneras:

1) Directamente del interesado.
2) A través de terceros, por una cesión legitima o de fuentes de acceso público.

En ambos casos, la empresa como **RTD** debe facilitar la siguiente información básica:

- ➔ La identidad del **RTD,** del **EPD** (si existe) y del **DPD**.
- ➔ La finalidad del tratamiento.
- ➔ La posibilidad de ejercer los derechos establecidos en la legislación.

Adicionalmente, en el supuesto 2) arriba indicado se incluirá también:

- ➔ Las categorías de datos objeto de tratamiento.
- ➔ Las fuentes de las que procedieran los datos.

Todos los derechos e informaciones que la legislación requiere sean comunicados a los interesados y que se desarrollan en los siguientes apartados, se recogen en nuestra **Política de Privacidad** (ver Anexo III), que es un documento que se encuentra accesible en nuestra página web y que debe ser actualizada por el **DPD** siempre que se produzcan cambios en los tratamientos, en las finalidades, en la información que allí aparece o cambios legislativos.

Por último, en nuestra Política de Privacidad se informará al interesado sobre el **plazo** durante el cual se conservarán los datos personales o al menos una idea aproximada de los plazos que la legislación establece. En particular los datos personales sólo se podrán conservar durante el tiempo necesario para la finalidad prevista. Si se extingue la autorización para el tratamiento de los mismos (se ha revocado el consentimiento o se ha cumplido el contrato), éstos deben eliminarse.

7.1. Derechos reconocidos

El **RTD** a través del **DPD** debe informar sobre los siguientes derechos que asisten a las personas interesadas, y que son:

- Derecho a solicitar el **acceso** del afectado a sus datos personales.
- Derecho a solicitar su **rectificación**.

- Derecho de **supresión** ("el derecho al olvido").
- Derecho a solicitar la **limitación** de su tratamiento.
- Derecho a **oponerse** al tratamiento.
- Derecho a la **portabilidad** de los datos.

Además de la enumeración de estos derechos se debe explicar al interesado el procedimiento para su ejercicio, facilitando una dirección de correo electrónico o bien se habilite un formulario electrónico.

Por último, se deberá informar a los interesados del derecho de presentar una **reclamación** ante la Autoridad de Control, en nuestro caso la **Agencia Española de Protección de Datos** (ver apartado 8), especialmente cuando no haya obtenido el interesado la satisfacción en el ejercicio de sus derechos, y la forma de ponerse en contacto con ella.

7.2 Información a los interesados

La obligación de informar a las personas interesadas sobre el tratamiento de sus datos recae sobre el **RTD**. Esta información se debe poner a disposición de los interesados en el momento en que se soliciten los datos previamente a la recogida o registro, si los datos se obtienen directamente del interesado.

En el caso de que los datos se obtengan a **través de terceros** se informará a los interesados dentro de un **plazo razonable**, pero en cualquier caso:

- Antes de un mes desde que se obtuvieron los datos personales.
- Antes o en la primera comunicación con el interesado.
- Antes de que los datos, en su caso, se hayan comunicado a otros destinatarios.

Esta obligación se debe cumplir **sin necesidad de requerimiento** alguno y nuestro DPD deberá poder acreditarlo con posterioridad que la obligación de informar ha sido satisfecha.

7.3 Información por capas

Para hacer compatible la exigencia de información que introduce la **LOPDGDD** y que a su vez sea concisa, transparente y con lenguaje claro y sencillo, optamos por una presentación por capas, es decir una información básica reducida y una información adicional más detallada.

La **información básica (1ª capa)** ya indicada, se presentará en la misma página web de recogida de datos, la cual remitirá a la **información adicional (2ª capa),** en un formato pdf, más adecuado para su consulta y archivo.

Ambos documentos constituyen la **Política de Privacidad** de nuestra empresa.

7.4 Consentimiento del interesado

Se entiende por consentimiento del interesado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de sus datos.

Para que el consentimiento sea **informado** es necesario comunicar al interesado ciertos elementos que son cruciales para poder elegir y que ya se han comentado anteriormente, en concreto:

-La identidad del **RTD**.

-El fin de cada una de las operaciones de tratamiento para las que se solicite el consentimiento.

-Qué tipo de datos van a recogerse y utilizarse.

-La existencia del derecho a retirar el consentimiento.

-Información sobre el uso de datos para decisiones automatizadas, cuando sea pertinente.

En el formulario de recogida de datos de nuestra página web se solicitará el **consentimiento explícito** para cada una de las finalidades definidas, mediante el marcado de las casillas correspondientes, no estando permitida la aceptación en bloque al aceptar la Política de. La solicitud del consentimiento se realizará de modo que no distraiga la atención del tratamiento de datos personales necesario para la ejecución de la relación que el interesado está contratando (p.ej.: uso de ventanas emergentes).

En el caso futuro que se tomen **decisiones automatizadas**, como la elaboración de perfiles, además de informar sobre este hecho en la Política de Privacidad, se debe explicar la lógica aplicada, la importancia que tiene para el interesado y las consecuencias que este tratamiento podría Privacidad tener para él.

8.-SEGURIDAD DE LOS DATOS E INCIDENCIAS.

8.1 Seguridad en la red

La seguridad en la red se entiende como la protección de información (documentos, datos bancarios, contraseñas,..) y datos personales en el entorno online. El principal objetivo es denegar el acceso a personas no autorizadas a los datos personales, evitando vulneraciones como la suplantación de identidad, software espía, phishing, virus o troyanos.

Los **mecanismos** utilizados en nuestra empresa son los siguientes:

Antivirus: Este tipo de protección permite evitar riesgos como la pérdida o daño de archivos, o la exposición de información confidencial a terceros.

Antispyware: Este programa impide el robo de datos impidiendo a su vez que los spyware ingresen y se instalen en nuestros ordenadores.

Firewall: Evita que los usuarios de Internet no autorizados tengan acceso a nuestra intranet. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

SAI (Sistema de Alimentación Ininterrumpida): Nos permite proporcionar a los equipos alimentación eléctrica cuando hay fallos en su suministro, y usar ese tiempo para almacenar correctamente los datos.

8.2 Control de acceso

El personal, ya sea propio o ajeno, sólo accederá a los datos y recursos que precise para el desarrollo de sus funciones y, por tanto, a aquéllos sobre los cuales se encuentra autorizado por el **DTD** mediante la **Lista de Usuarios y Perfiles,** así como de los accesos autorizados para cada uno de ellos.

Asimismo, establecerá mecanismos para evitar que un usuario pueda acceder a recursos con distintos derechos de los autorizados. En caso de soportes informáticos, consistirán en la asignación de **contraseñas** para acceder a los mismos, y, en caso de documentos, en la utilización de archivos físicos con llave u otro dispositivo equivalente. Dichas archivos deberán permanecer cerrados cuando no sea preciso el acceso a los documentos incluidos en el fichero.

A partir del momento mismo del **cese o cambio en el puesto de trabajo** de un usuario, se procederá a la actualización de la lista.

8.3 Locales y armarios

Los locales y armarios donde se ubiquen tanto los ordenadores como otros soportes físicos que contengan los datos deben ser objeto de **especial protección** que garantice la disponibilidad y confidencialidad de los mismos.

Los locales deberán contar con **medios de seguridad** que eviten los riesgos de indisponibilidad del Fichero que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.

El **acceso** a la zona donde se encuentren instalados los equipos físicos y lógicos que den soporte a los sistemas de información (servidores) deberá estar restringido exclusivamente a las personas autorizadas que deban realizar labores de mantenimiento para las que sean imprescindibles el acceso físico.

Mientras la documentación con datos de carácter personal **no se encuentre archivada** en los dispositivos de almacenamiento establecidos, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por personas no autorizadas.

8.4 Gestión de soportes y documentos

Dado que la mayor parte de los soportes que se utilizan (disquetes, CD, DVD, cintas o memorias flash o "pendrives"), así como todo tipo de documentación son fácilmente transportables, reproducibles y/o copiables, es evidente la **importancia** que para la seguridad de los datos del Fichero tiene el control de estos medios.

Los **soportes informáticos** que contengan datos de carácter personal, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo (backup) o cualquier otra operación esporádica, deberán estar **claramente identificados** con una etiqueta externa que indique de qué fichero se trata, o que tipo de datos contiene, proceso que los ha originado y fecha de creación.

Los **usuarios** que traten los soportes o documentos con datos de carácter personal son los encargados, en cada caso, de vigilar y controlar que personas no autorizadas no puedan acceder al soporte físico o documentos por ellos custodiados.

Cualquier soporte que vaya a ser **desechado**, de cualquier tipo, por haber sido dados de baja en el fichero, o por ser copias temporales, que pueda contener datos protegidos, ya sea documentos en papel impreso, o soportes informáticos, deberán ser tratados con el fin de impedir la pérdida de confidencialidad de los datos personales.

8.5 Puestos de trabajo

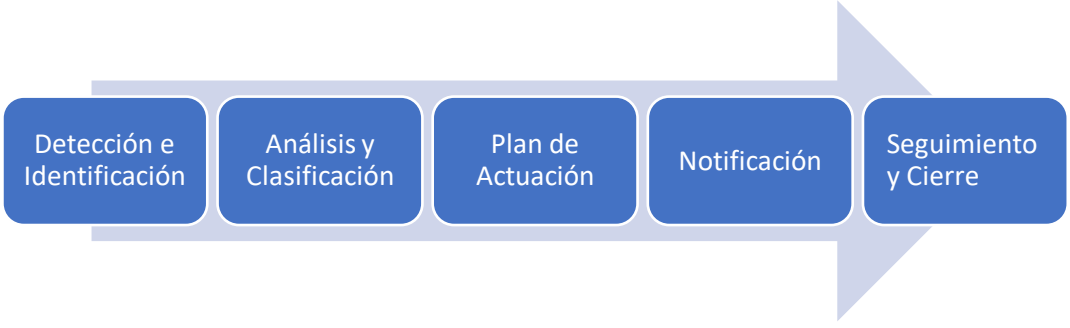
Cada puesto de trabajo está bajo la responsabilidad de un Usuario que garantizará que la información que muestra no pueda ser vista por personas no autorizadas. Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su jornada laboral, debe dejarlo en un estado que impida la visualización de los datos protegidos (p.ej.: a través de un protector de pantalla) y los documentos debidamente archivados.

8.6 Brechas de Seguridad

Nuestra empresa ha diseñado un **Plan de Contingencia** que se compone de los elementos ya indicados en los apartados anteriores, así como el disponer de una copia adicional de seguridad de la información de los PC y servidores en la nube.

Aun así cualquier empresa puede sufrir una brecha o incidencia de seguridad, entendiendo como tal todo suceso inesperado no deseado que ocasionen la destrucción, pérdida o alteración accidental o ilícita de los datos transmitidos, conservados o tratados de otra forma, o la comunicación o acceso por personas no autorizadas a dichos datos, siempre que puedan afectar a los derechos y libertades de las personas.

a. El establecer unos criterios para la gestión de estas incidencias nos permite garantizar la proactividad del RTD en sus actividades de tratamiento. La gestión conlleva las siguientes fases:



a. Detección e identificación.

La detección e identificación de un incidente de seguridad puede producirse a través de **fuentes internas** a nuestra empresa, ante el incumplimiento o vulneración de las medidas de seguridad adoptadas (p.ej.: bloqueo de pantallas, acceso con usuario o contraseña, controles de ciberseguridad, software antivirus, notificación de nuestros empleados, recepción de correos electrónicos con archivos sospechosos, robo o extravío de dispositivos de almacenamiento o equipos con información..), o a través de **fuentes externas** mediante la comunicación de un tercero (proveedor de servicios informáticos) por un Cliente, por órganos públicos de seguridad o incluso información publicada en medios de comunicación).

b. Análisis y clasificación.

El análisis de las fuentes anteriormente mencionadas permitirá determinar si se está ante un incidente de seguridad o no, así como su tipología, y si dicho incidente ha afectado a datos de carácter personal y, por tanto, constituye una violación de los datos descrita en la legislación, y el nivel de riesgo al que se enfrenta la empresa.

A continuación, se indican algunas tipologías de casos que pueden dar lugar a un incidente:

- ➔ Envío de e-mail con software malintencionado (malware).
- ➔ Inundación de tráfico en el servidor hasta que no sea capaz de dar servicio.
- ➔ Acceso a cuentas de usuario.
- ➔ Modificación de la página web (defacement).
- ➔ Robo/perdida de dispositivos de almacenamiento con información.

En función de estas tipologías, la brecha de seguridad se puede **clasificar**:

- ❑ **Brecha de confidencialidad**: Tiene lugar cuando partes que no están autorizadas para acceder a la información, acceden a ella.
- ❑ **Brecha de integridad**: Cuando se altera la información original y la sustitución de datos puede ser perjudicial para el interesado.

- **Brecha de disponibilidad**: Su consecuencia que no se puede acceder a los datos originales cuando es necesario. Puede ser temporal o permanente (los datos no pueden recuperarse).

Por último, el DPD debe realizar una valoración del alcance del incidente de seguridad en función de la peligrosidad del incidente y la estimación de la magnitud del impacto potencial en los ficheros afectados.

c. Plan de actuación.

El **RPD** y el **DPD**, junto con el asesoramiento de expertos en materia de seguridad, ya sean propios o subcontratados, y a la vista de la información recopilada y analizada sobre el incidente definirán un **Plan de Actuación** que incluya las acciones de respuesta a tomar, así como la notificación y/o comunicaciones oportunas según se indica en el apartado siguiente. También se valorará la posibilidad de poner el incidente en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado o de la Fiscalía, a través de una denuncia.

d. Notificación y/o comunicación.

Este apartado solo es aplicable en el caso que la incidencia de seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. En caso de ser aplicable, el **RTD** la notificará a la **AEPD** sin dilación indebida y como máximo dentro de las 72 horas después de que haya tenido constancia de ella. Para ello se utilizará el formulario que la **AEPD** ha dispuesto para ello (ver Anexo V).

Adicionalmente, el **RGPD** establece que, si la brecha de seguridad entraña un alto riesgo para los derechos y libertades de las personas físicas, el **RTD/DPD** deben comunicarlo a los interesados afectados.

e. Seguimiento y cierre.

Una vez las acciones derivadas del Plan de Actuación han concluido y se han alcanzado los objetivos se procederá al cierre de la incidencia de seguridad, mediante un informe final del **DPD** en el que se detalle la trazabilidad del suceso, vicisitudes, análisis valorativos e impacto final. Todos los documentos relacionados con el incidente constituirán un **Registro de Incidencias de Seguridad** (ver Anexo V), que debe ser conservado por el **DPD** por **tiempo ilimitado** a disposición de la **AEPD**.

9-RECLAMACIONES ANTE LA AEPD

La Autoridad de Control en España es la **Agencia Española de Protección de Datos**. La **AEPD** es una autoridad administrativa independiente de ámbito estatal que actúa con plena independencia de los poderes públicos en el ámbito de sus funciones.

Adicionalmente, la **LOPDGDD** prevé en su art.57 la existencia de **Autoridades Autonómicas de Protección de Datos** para aquellos tratamientos que se encuentren sometidos a su competencia, (aún no constituida en nuestra C. Autónoma).

La **AEPD** tiene la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.

En nuestra **Política de Privacidad** debe hacerse constar el derecho de los interesados a presentar una reclamación ante la Autoridad de Control, indicando la página web de contacto y/o el correo electrónico y/o el domicilio postal.

La tramitación de las reclamaciones de los interesados se regirá por lo indicado en el apartado 9.1 y los procedimientos tramitados por la **AEPD** por una posible vulneración de la normativa de protección de datos por lo indicado en el apartado 9.2.

Así mismo el **RTD** decidirá en un futuro la adhesión de **SMK** a **Códigos de Conducta** para la resolución de conflictos por parte por un Organismo o Entidad de Supervisión, tal y como se establece en el art.38 de la **LOPDGDD**.

9.1 Reclamaciones de los interesados

Toda reclamación relativa al tratamiento de datos que nos llegue a través de la dirección de correo electrónico indicada en nuestra Política de Privacidad o por cualquier otro medio escrito, será tratada y tramitada por el **DPD**, quién deberá comunicar al interesado la decisión que se haya adoptado en el **plazo máximo** de dos meses. Todas las reclamaciones se incluirán en un **Registro de Reclamaciones** (ver Anexo VI)

Puede darse el caso que el interesado haya presentado la reclamación directamente ante la **AEPD**, siendo habitual en este caso que la Agencia la remita al **RTD** o al **DPD** para que este responda en el plazo de un mes.

Una vez tramitada la reclamación y en el caso de que el interesado **no encontrase conforme** la decisión del **RTD**, aquel podrá dirigirse a la **AEPD** para resolver el conflicto.

9.2 Procedimientos tramitados por la AEPD

La **AEPD** podría iniciar en nuestra empresa un **procedimiento por vulneración** de la normativa de protección de datos en los siguientes supuestos:

a) Por falta de atención a una solicitud de un interesado del ejercicio de los derechos establecidos.

b) Por la posible existencia de una infracción de lo dispuesto en la **LOPDGDD** o en el **RGPD**, bien sea por propia iniciativa de la **AEPD** o como consecuencia de una reclamación.

c) Como consecuencia de la comunicación a la **AEPD** por parte de la autoridad de control de otro Estado Miembro de la UE de la reclamación formulada ante la misma.

En estos casos, el **RTD** a través del **DPD** deberá aportar a la **AEPD** todos aquellos documentos que se solicite, respetando los plazos de tramitación indicados para cada procedimiento.

9.3 Régimen sancionador

Con objeto de que todos los colaboradores de nuestra empresa tengan **conciencia de la importancia** de cumplir con lo indicado en la legislación, así como lo exigido por nuestro Sistema de Gestión, se incluyen los tipos de sanciones que se recogen en la **LOPDGDD** y en el **RGPD**. Como empresa debemos ser observantes y garantizar la protección de datos de nuestros Clientes, empleados y demás interesados.

a) **Sanciones muy graves**, las que supongan un incumplimiento sustancial del tratamiento. Se sancionarán con multas administrativas que pueden alcanzar los **20 millones de euros** o, tratándose de una empresa, de una cuantía equivalente al 4% de la facturación. (Plazo de prescripción: 3 años).
b) **Sanciones graves**, las que supongan una vulneración sustancial del tratamiento. Se sancionarán con multas administrativas que pueden ascender hasta los **10 millones de euros** o, si se trata de una empresa, una cuantía máxima del 2% de la facturación. (Plazo de prescripción: 2 años).
c) **Sanciones leves**, las restantes no contempladas en los apartados anteriores. Se determinarán en cada caso por la **AEPD** (Plazo de prescripción: 1 año).

El sujeto responsable de la sanción será el **RTD**. El **DPD no puede ser objeto** de sanción.

La lista completa de infracciones, así como el régimen sancionador se detalla en la **LOPDPGDD** en los artículos 70 al 78 y en los artículos 83 y 84 del RGPD.

10.-USO DE LAS COOKIES.

Las cookies son herramientas que tienen un papel esencial para la prestación de servicios en nuestra actividad ya que concentran la mayor inversión publicitaria para las empresas.

Las cookies son dispositivos de almacenamiento y recuperación de datos en los equipos terminales de los usuarios y por tanto tienen implicaciones importantes en relación con su privacidad. Se clasifican en:

- **Cookies propias:** aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio gestionado por **SMK** y desde el que se presta el servicio solicitado por el usuario.
- **Cookies de terceros**: aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio que no es gestionado por **SMK**, sino por otra entidad que trata los datos obtenidos través de las cookies.

Mediante la utilización de cookies en nuestra página web, obtendremos datos relacionados con los usuarios que posteriormente utilizaremos para la prestación de servicios concretos o como base para el desarrollo de mejoras o nuevos productos y servicios.

En relación con las cookies, nuestra empresa debe cumplir las obligaciones previstas, en el apartado segundo, del artículo 22 de la **LSSI**, además del **RGPD** y la **LOPDGDD**.

10.1 Tipos de cookies

Tanto las **cookies propias** creadas por nuestro sitio web como las **cookies de terceros** creadas por otros sitios web, tienen las siguientes finalidades:

- **Cookies técnicas**, que permiten al usuario la navegación a través de nuestra página web y la utilización de las diferentes opciones que en ella existen. Almacenan información genérica y anónima y no incluye datos de carácter personal.
- **Cookies de registro**, se crean con el registro de un usuario (log-in). Se utilizan para identificar al usuario una vez se ha autentificado dentro de la web.
- **Cookies de sesión**, que son necesarias para el correcto uso de la página, recomendando opciones de idioma o país. Se utilizan para identificar la sesión de navegación, midiendo así, por ejemplo la frecuencia.

- **Cookies analíticas**, que nos permiten el seguimiento y análisis del comportamiento de los usuarios y la cuantificación del impacto de los anuncios de nuestra página. Tienen una finalidad estadística utilizando la herramienta Google Analytics.
- **Cookies de publicidad comportamental**, que almacenan interacciones del comportamiento de los usuarios, lo que permite desarrollar un perfil específico para nuestras publicidades relacionadas con sus intereses o sus búsquedas anteriores. Algunas de estas cookies provienen de acuerdos que tienen con terceros.

10.2 Información de las cookies

La información que debemos facilitar a los usuarios sobre la utilización de las cookies debe ser clara y completa para permitir a los usuarios entender sus finalidades y el uso que se les dará. Nuestra **Política de Cookies** (ver Anexo VII) debe incluir, la siguiente información:

-Definición y función genérica de las cookies.

-Información sobre el tipo de cookies que se utilizan y su finalidad.

-Información sobre la forma de aceptar, denegar, revocar el consentimiento o eliminar las cookies.

-Si procede, información sobre la transferencia de datos a terceros países.

-Si procede, información sobre la elaboración de perfiles.

-Periodo de conservación de los datos.

- Referencia a la Política de Privacidad para el resto de información sobre derechos de los interesados.

El lenguaje utilizado en nuestra Política de Cookies debe ser claro y sencillo, de forma que pueda ser entendida por un usuario medio, evitando el uso de frases que induzcan a confusión o desvirtúen la claridad del mensaje.

El acceso a la información se proporciona en nuestra página web a través de un enlace claramente visible que dirige directamente a nuestra ***"Política de Cookies",*** en la base de nuestra página. Esta zona de ubicación es práctica habitual y de uso generalizado, ayudando a garantizar la accesibilidad y visibilidad.

10.3 Obtención del consentimiento

La información se facilita antes del uso de las cookies, incluida su instalación, a través del siguiente formato, que permanece visible en la página web hasta que el usuario realice la acción requerida para su consentimiento o rechazo.

. **Uso de cookies**

Este Sitio Web utiliza cookies propias y de terceros para fines analíticos y para mostrarte publicidad personalizada en base a un perfil elaborado a partir de tus hábitos de navegación. Para más información, haz clic AQUÍ. Puedes aceptar todas las cookies pulsando el botón "ACEPTAR" o configurarlas o rechazarlas su uso clicando en nuestra Política de Cookies.

ACEPTAR

En consecuencia, la utilización de las cookies tendrá lugar cuando el usuario disponga de la información preceptiva y tenga la oportunidad de examinar la información y decidir si aceptan o no su utilización.

10.4 Cambios en el uso de cookies

Teniendo en cuenta los posibles cambios que se puedan producir en la gestión y uso de las cookies, el **DPD** realizará anualmente una revisión a fin de actualizar, si procede, la información disponible sobre estas. Esta revisión se centrará en:

-Comprobar si se han producido cambios normativos.

-Comprobar las cookies que se están utilizando, analizando si son propias o de terceros y confirmando su función.

En el caso de que se produjeran cambios será necesario permitir a los usuarios tomar una nueva decisión.

11.-EVALUACIÓN, ANÁLISIS Y MEJORA

11.1 Evaluación del Sistema

Anualmente el **RTD** designará a una **empresa independiente** que acredite disponer de personal con conocimientos especializados en el derecho y la práctica en materia de protección de datos para la evaluación del **SGSTDP**.

Los resultados del informe emitido por el evaluador se tendrán en cuenta a la hora establecer acciones de mejora.

11.2 Análisis y Mejora

El **RTD** junto con el **DPD** analizaran todos los hechos relevantes que se produzcan anualmente en el **SGSTDP**, en particular los siguientes:

-Reclamaciones e incidencias de seguridad.

-Solicitudes de derechos ejercidos por los interesados y su tramitación.

-Existencia de procedimientos abiertos por la **AEPD** y su estado de tramitación.

-Si procede, tramitación de casos en la Autoridad de Resolución de Conflictos

-Cambios en los sistemas informáticos.

-Cambios organizativos.

-Cambios en los ficheros de datos y/o en el tratamiento.

-Resultados del informe de la evaluación anual.

-Cambios legislativos que puedan afectar a nuestro Sistema, a nuestra Política de Privacidad y/o Política de Cookies.

Del resultado del análisis se dejará constancia en un **Informe de Análisis de Sistema**, en el que incluirán además las acciones de mejora que se determinen para llevarlas a cabo en el siguiente período.

12.-CONCLUSIONES.

El desarrollo del presente trabajo me ha permitido estudiar con profundidad el **derecho a la protección de los datos de carácter personal** recogido en la Carta de los Derechos Fundamentales de la Unión Europea y posteriormente desarrollado en la legislación europea y española.

Así mismo he consultado numerosas **fuentes bibliográficas**, principalmente publicaciones de la Agencia Española de Protección de Datos, del Instituto Nacional de Ciberseguridad, Asociaciones de Marketing y Publicidad, artículos y blogs en internet, páginas web de Agencias de Marketing Online, todo ello relacionado con el Marketing Online, con la Seguridad de las TIC´s y con la Protección de Datos.

Personalmente la realización de este trabajo ha sido una experiencia muy enriquecedora para **conocer en profundidad** como puede gestionarse con eficacia la seguridad y la privacidad en el Marketing Online, tratando de establecer un puente entre la legislación aplicable y un sistema de gestión que facilite a las empresas su cumplimiento.

Además, la realización de las prácticas de grado en el departamento de marketing de una empresa, me ha ayudado para tener una **visión global** sobre el tratamiento de los datos. Tuve la oportunidad de poder asistir a varias reuniones con la empresa externa como Encargada del Tratamiento de Datos y que fue de gran ayuda para comprender los conceptos de seguridad y privacidad.

Del resultado de este trabajo y de la extensa información que he consultado y leído veo el amplio campo que se me abre en el Marketing Digital (en el que estoy dispuesto a profundizar), con las **nuevas tendencias** como el Mindful marketing (escuchar para generar acciones y soluciones personalizables), la llegada del 5G y de la Inteligencia Artificial (IA) para crear nuevos métodos, el auge de las web’s comparadoras, un nuevo modelo de web basado en el relato, la TV-commerce o las nuevas formas de colaboración entre los influencers y las marcas. Como resultado de todo ello también se prevén **cambios en la legislación** nacional, como el Reglamento Europeo de e-Privacy que se está desarrollando, o la transposición a derecho interno de la Directiva 2019/770, de servicios digitales.

13.-BIBLIOGRAFÍA

- **Informe sobre políticas de privacidad en internet. Adaptación al RGPD.**
  AEPD (Agencia de Protección de Datos). Octubre 2018.
- **LOPD: Novedades para los ciudadanos**.
  AEPD (Agencia de Protección de Datos). Diciembre 2018.
- **Guía para el ciudadano.**
  AEPD (Agencia de Protección de Datos). Febrero 2019.
- **LOPD: Novedades para el sector privado.**
  AEPD (Agencia de Protección de Datos). Marzo 2019.
- **Guía práctica de análisis para el Tratamiento de Datos Personales.**
  AEPD (Agencia de Protección de Datos). Junio 2019.
- **Guía sobre el uso de las Cookies.**
  AEPD, IAB Spain y otros. Noviembre 2019.
- **Guía de Privacidad desde el Diseño.**
  AEPD (Agencia de Protección de Datos). Noviembre 2019.
- **Guía Práctica de análisis de riesgos en los Tratamientos de Datos Personales.**
  AEPD (Agencia de Protección de Datos).
- **Guía Práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD**
  AEPD (Agencia de Protección de Datos).
- **Guía para la gestión y notificación de brechas de seguridad.**
  INCIBE/AEPD (Agencia de Protección de Datos). Junio 2018.
- **Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento.**
  AEPD/Agencia Catalana de Protección de Datos/Agencia Vasca de Protección de Datos. Mayo 2018.
- **Guía para el cumplimiento del deber de informar.**
- AEPD/Agencia Catalana de Protección de Datos/Agencia Vasca de Protección de Datos. Mayo 2018.

14.-ANEXOS

Anexo I. Tabla de Equivalencias del Sistema de Gestión y Legislación.

Anexo II. Registro de Actividades de Tratamiento de Datos.

Anexo III. Política de Privacidad (Resumida y Detallada)

Anexo IV. Formulario de Notificación a la AEPD

Anexo V. Registro de Incidencias de Seguridad.

Anexo VI. Registro de Reclamaciones.

Anexo VII. Política de Cookies.

ANEXO I.- TABLA DE EQUIVALENCIAS DEL SISTEMA Y LEGISLACIÓN.

APARTADO SGSTDP	DESCRIPCIÓN	ARTÍCULO LOPDGDD	ARTÍCULO RGPD
1	INTRODUCCIÓN	--	--
2	LEGISLACIÓN APLICABLE	--	--
3	DEFINICIONES Y ABREVIATURAS	--	Art. 4
4	DECLARACIÓN SOBRE PRIVACIDAD	Art.4	Art.5
5	SISTEMA DE GESTIÓN DE LA SEGURIDAD	Art.2.1, 5.1. Art. 28, 34, 36	Art.2.1 Art.24, 25, 28, 29.
6	TRATAMIENTO DE LOS DATOS	Art.3, 6÷9, 31, 32. Art. 40÷43	Art.5÷9, 30, 35 Art. 44÷49
7	DERECHOS E INFORMACIÓN A LOS INTERESADOS	Art. 11÷19	Art.12÷22
8	SEGURIDAD DE LOS DATOS E INCIDENCIAS	--	Art.32, 33÷34
9	RECLAMACIONES ANTE LA AEPD	Art.38, 44÷62 Art.63÷78	Art.51÷59 Art.83, 84
10	USO DE LAS COOKIES	Art.6	Art.4, 13
11	EVALUACIÓN, ANÁLISIS Y MEJORA	--	--
12	CONCLUSIONES	--	--

ANEXO II.-REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE DATOS.

Smarketing4ALL **AGENCIA DE MARKETING**	**REGISTRO DE TRATAMIENTO DE DATOS.** ☐ **CLIENTES** ☐ **CLIENTES POTENCIALES** ☐ **PROVEEDORES** ☐**RR.HH**	**Registro Nº:** **Fecha: Junio 2020**

RESPONSABLE DEL TRATAMIENTO

Razón Social: **Smarketing4all, S.L**
Dirección: Centro ETOPIA. Avda. Ciudad de Soria, 8. 50010 Zaragoza.
Datos de contacto del RTD:
CIF:
Email: smarketing4all@smarketing.com
Teléfono:
Datos de contacto del DPD:
Email: lopdp@smarketing.com
Encargado del Tratamiento de Datos: No hay

DESCRIPCIÓN DE LA ACTIVIDAD DE TRATAMIENTO (*)

Descripción:
Finalidad:
Proceso de Captura de Datos: ☐ Sistema informático ☐ Manual ☐ Otros (indicar).
Categorías Datos Tratados: ☐ Identificativos ☐ Financieros ☐ Salud ☐ Otros (Indicar)
Interesados: ☐Clientes ☐Personas de contacto ☐Proveedores ☐Empleados ☐Otros (indicar).
Tecnología: ☐ Sistema informático ☐ Manual
Proceso de solicitud del consentimiento: ☐ Sitio Web ☐ Formulario
Cesiones: ☐ Empresa Informática ☐ Gestoría ☐ Admón. Pública ☐ Otros (Indicar)
Transferencias previstas: No se realizan transferencias internacionales fuera del EEE.
Plazo de Conservación:
(*) Rellenar lo mismo para cada tratamiento realizado: Clientes, Proveedores, RR. HH...

ESTRUCTURA BÁSICA Y DESCRIPCIÓN DE LOS TIPOS DE DATOS

Carácter identificativo (**):

Datos protegidos: ☐ **NO** ☐**SI** (Indicar)

Otros datos tipificados (***):

(**) P.Ej.: Nombre, apellidos, cif/nif, email, teléfono, fax.
(***) P.Ej.: información comercial, económicos, financieros,..

ALMACENAMIENTO DE LOS DATOS Y MEDIDAS DE SEGURIDAD

Información almacenada en: ☐Sistema Informático ☐Archivo físico nº:_____
Copia de respaldo y procedimiento de recuperación:
Intervinientes: Empleados del departamento de:_____

Responsable de Seguridad:

Otras medidas técnicas y organizativas de seguridad (*):

(*) Indicar los programas de protección y medidas físicas de seguridad.

El Registro de Actividades de Tratamiento debe guardarse en la empresa y tenerlo siempre **actualizado y a disposición de la Autoridad de Control (AEPD)**, si ésta nos lo solicita.

ANEXO III.-POLÍTICA DE PRIVACIDAD.

EPIGRAFE	INFORMACIÓN BÁSICA (1ª capa resumida)	POLÍTICA DE PRIVACIDAD DE Smrketing4All, S.L. (1ª capa resumida. Versión 06.2020)
RESPONSABLE DEL TRATAMIENTO.	**Identidad del RTD.**	**Smarketing4all, S. L.**
FINALIDAD DEL TRATAMIENTO	**Descripción sencilla de los fines del tratamiento**	**F1: Atender la solicitud de información de los Usuarios** **F2: Mantener informado al Usuario acerca de nuestros servicios** **F3: Posibilitar la participación del Usuario en las actividades propuestas y descarga de contenidos gratuitos.** **No se utilizan los datos para la toma de decisiones automatizadas ni elaborar perfiles.**
LEGITIMACIÓN.	**Base jurídica del tratamiento**	**F1: Consentimiento del interesado.** **F2: Consentimiento del interesado.** **F3: Consentimiento del interesado.**
DESTINATARIOS **(de cesiones o transferencias)**	**-Previsión o no de cesiones.** **-Previsiones de transferencias, o no, a terceros países.**	**-Los datos podrán cederse a Administraciones Públicas, a empresas informáticas, gestorías y a clientes de actividades del comercio.** **-No hay transferencia de datos a países fuera del Espacio Económico Europeo.**
DERECHOS **(de los usuarios)**	**Referencia al ejercicio de derechos.**	**El Usuario puede ejercer ante Smarketing4All sus derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, oposición y a no ser objeto de decisiones individuales incluidas la elaboración de perfiles.** **En todo caso el Usuario tiene derecho a presentar una reclamación ante la Autoridad de Control (https://www.aepd.es).**
PROCEDENCIA **(si no proceden del Usuario)**	**Fuente de los datos.**	**Los datos que tratamos proceden exclusivamente de los interesados.**

Si desea más información detallada pulse AQUÍ

ANEXO III.-POLÍTICA DE PRIVACIDAD. (CONT.)

EPIGRAFE	INFORMACIÓN BÁSICA (2ª capa detallada)	POLÍTICA DE PRIVACIDAD DE Smrketing4All, S.L. (2ª capa detallada. Versión 06.2020)
RESPONSABLE DEL TRATAMIENTO.	**Identidad y datos de contacto del RTD y del DPD**	**Razón Social**: Smarketing4all, S.L **Dirección:** Centro ETOPIA. Avda. Ciudad de Soria, 8. 50010 Zaragoza. **Email RTD:** smarketing4all@smarketing.com **Email DPD**: lopdp@smarketing.com
FINALIDADES DEL TRATAMIENTO	**-Descripción ampliada de los fines del tratamiento. -Plazos o criterios de conservación de los datos. -Decisiones automatizadas, perfiles y lógica aplicada**	**F1: Atender la solicitud de información de los Usuarios. Los datos se conservarán hasta haber dado respuesta a la solicitud de información. F2: Mantener informado al Usuario acerca de nuestros productos, servicios y novedades. Los datos se conservarán la revocación del consentimiento. F3: Posibilitar la participación del Usuario en las actividades propuestas y descarga de contenidos gratuitos. También se utilizarán los datos para mantenerle informado de productos, servicios y novedades de terceras personas exclusivamente pertenecientes a los sectores de moda, deportes, alimentación y bebidas. Los datos se conservarán hasta que el Usuario revoque su consentimiento.**
LEGITIMACIÓN.	**Base jurídica del tratamiento, en casos de obligación legal, interés público o legítimo.**	**F1: Consentimiento del interesado. F2: Consentimiento del interesado. F3: Consentimiento del interesado.**
DESTINATARIOS (de cesiones o transferencias)	**Destinatarios o categorías de destinatarios.**	**-Los datos podrán comunicarse a los siguientes destinatarios de terceros: Administraciones Públicas para el cumplimiento de obligaciones legales, a empresas de mantenimiento informático, gestorías y a empresas pertenecientes a los sectores de actividad vinculados a la finalidad nº3.No hay transferencia de datos a países fuera del Espacio Económico Europeo.**
DERECHOS (de los usuarios)	**-Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento. -Derecho a retirar el consentimiento prestado.**	**El Usuario puede ejercer ante Smarketing4All sus derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, oposición y a no ser objeto de decisiones individuales incluidas la elaboración de perfiles. Puede retirar en cualquier momento el consentimiento previo otorgado. Adicionalmente el Usuario puede presentar una Reclamación ante la Agencia Española de Protección de Datos (www.aepd.es).**
PROCEDENCIA (si no proceden del Usuario)	**-Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público. -Categorías de los datos que se traten.**	**-Los datos que tratamos proceden exclusivamente de los interesados. -No se tratan datos especialmente protegidos.**

ANEXO IV.- FORMULARIO DE NOTIFICACIÓN A LA AEPD.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

1. Datos de la notificación

Tipo de notificación: ○ Inicial, ○ Adicional, ○ Completa
Referencia notificación inicial:_____ Fecha notificación inicial:_____

2. Identificación del Delegado de Protección de Datos o persona de contacto

NIF/NIE: _____ Nombre:_____
Apellidos:_____ Cargo:_____
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

3. Identificación del responsable del tratamiento

Nombre de la Organización: _____
Tipo de Organización: ○ Privada, ○ Pública
CIF:_____ Dirección distinta del DPD o persona de contacto: ☐
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

4. Identifiación del encargado del tratamiento

¿Hay otra organización implicada en la brecha de seguridad? ☐
Nombre de la Organización: _____
Tipo de Organización: ○ Privada, ○ Pública
CIF:_____
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

5. Información temporal de la brecha

Fecha detección de la brecha: _____ ○ Exacta, ○ Estimada.
Medios de detección de la brecha:

_____
_____
_____

Justificación de notificación tardía (notificación pasadas 72h desde la detección):

_____
_____
_____

Fecha inicio de la brecha: _____ ○ Exacta, ○ Estimada.
¿Está resuelta la brecha? ☐ Fecha de resolución: _____ ○ Exacta, ○ Estimada.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

6. Sobre la brecha

Resumen del incidente:

Tipología:

- ☐ Brecha de confidencialidad (acceso no autorizado)
- ☐ Brecha de integridad (modificación no autorizada)
- ☐ Brecha de disponibilidad (desaparición o pérdida)

Medio por el que se ha materializado la brecha:

- ☐ Datos personales residuales en dispositivos obsoletos.
- ☐ Documentación perdida, robada o depositada en localización insegura.
- ☐ Eliminación incorrecta de datos personales en formato papel.
- ☐ Hacking.
- ☐ Malware (e.j. ransomware).
- ☐ Phishing.
- ☐ Correo perdido o abierto.
- ☐ Dispositivo perdido o robado.
- ☐ Publicación no intencionada.
- ☐ Datos personales mostrados al individuo incorrecto.
- ☐ Datos personales enviados por error.
- ☐ Revelación verbal no autorizada de datos personales.
- ☐ Otros: _____

Contexto:

- ○ Interna (acción no intencionada)
- ○ Externa(acción no intencionada)
- ○ Otros:
- ○ Interna (acción intencionada)
- ○ Externa (acción intencionada)

Medidas preventivas aplicadas antes de la brecha:

7. Sobre los datos afectados

Categoría de datos afectados:

- ☐ Datos básicos
- ☐ Credenciales de acceso o identificación
- ☐ Datos de contacto
- ☐ DNI, NIE y/o Pasaporte
- ☐ Datos económicos o financieros
- ☐ Datos de localización
- ☐ Sobre condenas e infracciones penales
- ☐ Otros: _____

C/ Jorge Juan, 6 28001 Madrid www.agpd.es

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

Categorías especiales de datos:

☐ Sobre el orígen racial ☐ Sobre la opinión política
☐ Sobre la religión o creencia ☐ Sobre la afiliación sindical ☐ Sobre la vida sexual
☐ De salud ☐ Genéticos ☐ Biométricos
☐ Desconocidos ☐ Otros: _____

Número aproximado de registros de datos personales afectados:

8. Sobre los sujetos afectados

Perfil de los sujetos afectados:

☐ Clientes ☐ Usuarios ☐ Empleados ☐ Suscriptores
☐ Estudiantes ☐ Pacientes ☐ Otros: _____

Número aproximado de personas afectadas:

9. Posibles consecuencias

Brecha de confidencialidad:

☐ Divulgación a terceros /difusión en internet ☐ Los datos pueden ser explotados con otros fines
☐ Enriquecimiento de otras bases de datos ☐ Otras: _____

Brecha de integridad:

☐ Datos han sido modificados aunque hayan quedado inservibles o irrecuperables ☐ Datos han sido modificados y utilizados para otros fines
☐ Otras: _____

Brecha de disponibilidad:

☐ Imposibilidad de la prestación de un servicio a los interesados ☐ Deterioro de las condiciones de prestación de un servicio a los interesados
☐ Otras: _____

Naturaleza del impacto potencial sobre los sujetos:

☐ Pérdida de control sobre sus datos personales ☐ Limitación de sus derechos ☐ Discriminación
☐ Usurpación de identidad ☐ Fraude ☐ Pérdidas financieras
☐ Reidentificación no autorizada ☐ Perdida de confidencialidad de datos afectados por secreto profesional
☐ Daños a la reputación ☐ Otras: _____

Severidad de las consecuencias para los individuos: ○ Baja ○ Media ○ Alta ○ Muy alta

Medidas tomadas para solucionar la brecha y minimizar el impacto sobre los afectados:

_____
_____
_____
_____
_____

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

10. Comunicación a los interesados

¿Se ha comunicado la brecha a los interesados?

○Si — Fecha en la que se informó: _____

Número de sujetos informados: _____

Medios o herramientas de comunicación: _____

○No, pero serán informados — Fecha en la que se informará: _____

○No serán informados — Justificación para no informar: _____

○Pendiente de decidir

(Adjuntar contenido de la comunicación a los interesados)

11. Implicaciones trasfronterizas

¿Hay sujetos de otros Estados miembros de la UE afectados por la brecha? ☐

Marque los Estados que puedan estar afectados (A) y aquellos a los que haya notificado(N) la misma brecha de seguridad:

A	N		A	N		A	N	
☐	☐	Alemania	☐	☐	Austria	☐	☐	Bélgica
☐	☐	Bulgaria	☐	☐	Chipre	☐	☐	Croacia
☐	☐	Dinamarca	☐	☐	España	☐	☐	Eslovaquia
☐	☐	Eslovenia	☐	☐	Estonia	☐	☐	Finlandia
☐	☐	Gran Bretaña	☐	☐	Grecia	☐	☐	Hungría
☐	☐	Irlanda	☐	☐	Italia	☐	☐	Letonia
☐	☐	Lituania	☐	☐	Luxemburgo	☐	☐	Malta
☐	☐	Países Bajos	☐	☐	Polonia	☐	☐	Portugal
☐	☐	Rep. Checa	☐	☐	Rumania	☐	☐	Suecia

12. Documentos adjuntos

(Adjuntar documentos)

En_____,a___de_____20__

C/ Jorge Juan, 6 — 28001 Madrid — www.agpd.es

ANEXO V.- REGISTRO DE INCIDENCIAS DE SEGURIDAD

Smarketing4ALL **AGENCIA DE MARKETING**	**REGISTRO DE INCIDENCIAS DE SEGURIDAD PROTECCIÓN DE DATOS PERSONALES**	**Código Nº:** **Fecha :**

DETECCIÓN E IDENTIFICACIÓN

DESCRIPCIÓN DEL INCIDENTE: (Indicar las medidas de seguridad que se han vulnerado si provienen de fuentes internas o externas a la empresa.

REPONSABLES DEL ANÁLISIS: DPD + ……

ANÁLISIS Y CLASIFICACIÓN

(Indicar la tipología, valoración del alcance y la clasificación de la brecha)

☐**BRECHA DE CONFIDENCIALIDAD** ☐**DE INTEGRIDAD** ☐ **DE DISPONIBILIDAD**

¿REQUIERE AYUDA EXTERNA?: ☐ **SI (Indicar).** ☐ **NO.**
¿REQUIERE NOTIFICACIÓN A LOS INTERESADOS?:☐**SI** ☐ **NO.**
¿REQUIERE NOTIFICACIÓN A LA AEPD?: ☐ **SI (Antes de 72h.)** ☐ **NO.**

CAUSAS

(Indicar, si se conocen, las causas que han producido el incidente)

PLAN DE ACTUACIÓN

	RESPONSABLE	**FECHA**
1.-		
2.-		
3.- (En caso necesario ampliar en anexo aparte)		

SEGUIMIENTO Y CIERRE

(Se realizará un informe final por el DPD)

INFORME FINAL DE LA INCIDENCIA Nº……**FECHA**:……..

ANEXOS: Se anexarán a este registro toda la documentación generada y que debe ser conservada por tiempo **ilimitado** a disposición de la AEPD.

Fecha de Cierre:	**Responsable del cierre:** DPD

ANEXO VI.- REGISTRO DE RECLAMACIONES

Smarketing4ALL AGENCIA DE MARKETING	REGISTRO DE RECLAMACIÓN PROTECCIÓN DE DATOS PERSONALES	Código Nº:
		Fecha Recepción:

DATOS DEL INTERESADO

NOMBRE/RAZÓN SOCIAL: **EMAIL:**

SI PROCEDE, ¿REMITIDA POR LA AEPD?: ☐ **SI** ☐ **NO**

RESPONSABLE DE TRAMITACIÓN: **TRAMITAR ANTES DE:**_____

DESCRIPCIÓN DE LA RECLAMACIÓN

(Descripción del derecho solicitado por el interesado)

CAUSAS

(Indicar las causas que motivan la reclamación, si procede)

ACCIONES A TOMAR

	RESPONSABLE	FECHA
1.-		
2.-		
3.-		

COMPROBACIÓN DE LAS ACCIONES Y CIERRE

NOTIFICACIÓN AL INTERESADO: ☐ **EMAIL (Fecha:……)**

ANEXOS: Se anexarán a este registro toda la documentación recibida del interesado o de la AEPD, así como de las acciones tomadas y de la comunicación del cierre de la reclamación

Fecha de Cierre:	Responsable del cierre:

ANEXO VII.- POLÍTICA DE COOKIES

Smarketing4ALL AGENCIA DE MARKETING	POLÍTICA DE COOKIES	Versión:0 Pág. 1 de 2
		Fecha: Junio 2020

En cumplimiento con lo dispuesto en el artículo 22.2 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, esta página web le informa, en esta sección, sobre la política de recogida y tratamiento de cookies.

¿Qué son las cookies?

Una ***cookie*** es un fichero que se descarga en su ordenador al acceder a determinadas páginas web. Las cookies permiten a una página web, entre otras cosas, almacenar y recuperar información sobre los hábitos de navegación de un usuario o de su equipo. Estas tecnologías son esenciales para el correcto funcionamiento, integridad, disponibilidad y pertinencia de los contenidos de este Sitio Web, y aportan importantes ventajas en la prestación de los servicios, facilitando la navegación y usabilidad. Las cookies no pueden leer informaciones almacenadas en ningún terminal. Tampoco pueden dañar ni alterar su equipo.

Las ***cookies*** utilizadas en nuestro Sitio Web son propias y de terceros y nos permiten almacenar y acceder a información relativa al idioma, el tipo de navegador utilizado y a otras características generales predefinidas por el usuario, así como seguir y analizar la actividad que lleva a cabo, con el objeto de introducir mejoras y prestar nuestros servicios de una manera más eficiente y personalizada.

Qué tipos de cookies utiliza esta página web?

Cookies técnicas, que permiten al usuario la navegación a través de nuestra página web y la utilización de las diferentes opciones que en ella existen.

Cookies de registro, se crean con el registro de un usuario (log-in). Se utilizan para identificar al usuario una vez se ha autentificado dentro de la web.

Cookies de sesión, que son necesarias para el correcto uso de la página, recomendando opciones de idioma o país. Las cookies de sesión son memorizadas y únicamente tienen validez temporal, es decir, hasta que el usuario finaliza la navegación por la página web. Estas cookies no graban de forma permanente ninguna información en el disco duro de su ordenador.

Cookies analíticas, que nos permiten el seguimiento y análisis del comportamiento de los usuarios y la cuantificación del impacto de los anuncios de nuestra página.

Cookies de publicidad comportamental, que almacenan interacciones del comportamiento de los usuarios, lo que permite desarrollar un perfil específico para nuestras publicidades relacionadas con sus intereses o sus búsquedas anteriores. Algunas de estas cookies provienen de acuerdos que tenemos con terceros.

ANEXO VII.- POLÍTICA DE COOKIES (CONT.)

Smarketing4all AGENCIA DE MARKETING	POLÍTICA DE COOKIES	Versión:0 Pág. 2 de 2
		Fecha: Junio 2020

Cómo desactivar las Cookies

Puede usted permitir, bloquear o eliminar las cookies instaladas en su equipo mediante la configuración de las opciones del navegador instalado en su ordenador.

A continuación, puede acceder a la configuración de los navegadores webs más frecuentes para aceptar, instalar o desactivar las cookies:

•Microsoft Internet Explorer o Microsoft Edge: http://windows.microsoft.com/es-es/windows-vista/Block-or-allow-cookies.

•Mozilla Firefox: http://support.mozilla.org/es/kb/impedir-que-los-sitios-web-guarden-sus-preferencia.

•Chrome: https://support.google.com/accounts/answer/61416?hl=es.

•Safari: http://safari.helpmax.net/es/privacidad-y-seguridad/como-gestionar-las-cookies/.

Cookies de Terceros

Esta página web utiliza servicios de terceros para recopilar información con fines estadísticos y de uso de la web. En concreto, usamos los servicios de Google Analytics y Google Adsense para nuestras estadísticas y publicidad. El usuario podrá excluir su actividad individual mediante los sistemas de exclusión facilitado por Google.

Destruiremos los datos de carácter personal cuando nos lo requiera expresamente y por escrito.

Para conocer los derechos que le asisten pulse nuestra *Política de Privacidad*